

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11213552 A**

(43) Date of publication of application: 06.08.99

(51) Int. Cl.

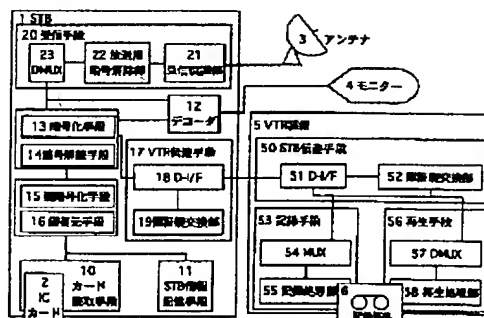
G11B 20/10**G09C 1/00****H04L 9/08**(21) Application number: **10012474**(22) Date of filing: **26.01.98**(71) Applicant: **MATSUSHITA ELECTRIC IND CO LTD**(72) Inventor: **YAMADA MASAZUMI
IIZUKA HIROYUKI
GOTO SHOICHI
TAKECHI HIDEAKI**(54) **DATA RECORDING/REPRODUCING METHOD
AND DATA RECORDING/ REPRODUCING
METHOD**

COPYRIGHT: (C)1999,JPO

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a data recording and reproducing system by which reproduction can be performed only for a specific object and information about coding is hard to leak to the outside.

SOLUTION: This device is provided with a receiving means 20 receiving digital data, a ciphering means 13 generating a work key, ciphering the digital data using the work key, and generating coded digital data, a key ciphering means 15 performing a second ciphering for the work key and generating a ciphered work key, a recording means 53 recording the ciphered digital data and the ciphered work key in a key recording means 6, a reproducing means 56 reproducing the ciphered signal data and the ciphered work key from the recording medium 6, a key restoring means 16 decoding the ciphered work key and restoring the work key, and a deciphering means 14 decoding the ciphered digital data using the restored work key and obtaining the digital data.



引用例2の写し

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-213552

(43) 公開日 平成11年(1999) 8月6日

(51) Int.Cl.⁸
G 1 1 B 20/10
G 0 9 C 1/00
H 0 4 L 9/08

識別記号
6-6 0

F I
G 1 1 B 20/10
G 0 9 C 1/00
H 0 4 L 9/00
H
6 6 0 G
6 6 0 D
6 0 1 E
6 0 1 A

審査請求 未請求 請求項の数38 O L (全 29 頁)

(21) 出願番号 特願平10-12474

(22) 出願日 平成10年(1998) 1月26日

(71) 出願人 000005821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 山田 正純

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72) 発明者 飯塚 裕之

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(72) 発明者 後藤 昌一

大阪府門真市大字門真1006番地 松下電器産業株式会社内

(74) 代理人 弁理士 松田 正道

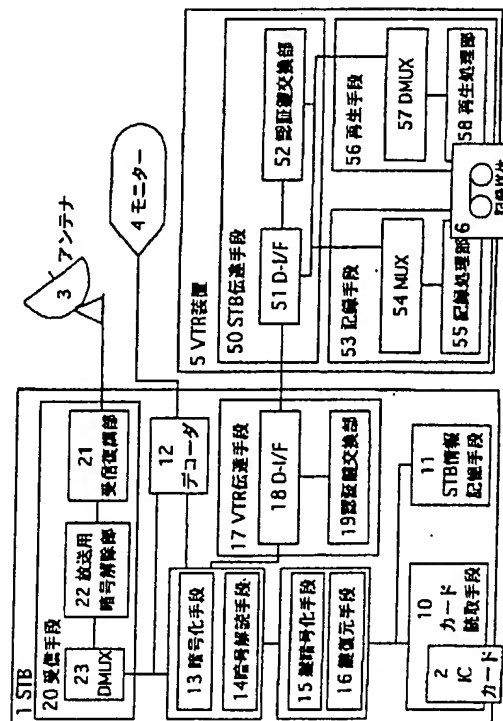
最終頁に続く

(54) 【発明の名称】 データ記録再生方法およびデータ記録再生システム

(57) 【要約】

【課題】 特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムを提供する。

【解決手段】 デジタルデータを受信する受信手段20と、ワークキーを生成し、前記デジタルデータに前記ワークキーを用いて暗号化を施して暗号化デジタルデータを生成する暗号化手段13と、前記ワークキーに第2の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段15と、前記暗号化デジタルデータおよび前記暗号化ワークキーを記録媒体6に記録する記録手段53と、記録媒体6から前記暗号化デジタルデータおよび前記暗号化ワークキーを再生する再生手段56と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段16と、復元された前記ワークキーを用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得る暗号解読手段14とを備える。



【特許請求の範囲】

【請求項1】 デジタルデータにワークキーを用いて第1の暗号化を施した暗号化デジタルデータと、前記ワークキーに第2の暗号化を施した暗号化ワークキーとを記録媒体に記録し、記録された前記暗号化デジタルデータおよび前記暗号化ワークキーを再生し、前記暗号化ワークキーを解読して得られた前記ワークキーを用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得ることを特徴とするデータ記録再生方法。

【請求項2】 前記暗号化ワークキーを、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項1に記載のデータ記録再生方法。

【請求項3】 前記ワークキーを、定期的または不定期的に切り替えることを特徴とする請求項1または2に記載のデータ記録再生方法。

【請求項4】 外部からデジタルデータを受信する受信手段と、ワークキーを生成し、前記デジタルデータに前記ワークキーを用いて第1の暗号化を施して暗号化デジタルデータを生成する暗号化手段と、前記ワークキーに第2の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段と、前記暗号化デジタルデータおよび前記暗号化ワークキーを記録媒体に記録する記録手段と、前記記録媒体から前記暗号化デジタルデータおよび前記暗号化ワークキーを再生する再生手段と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段と、復元された前記ワークキーを用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得る暗号解読手段とを備えることを特徴とするデータ記録再生システム。

【請求項5】 前記全ての手段は、一体化された装置に備えられていることを特徴とする請求項4に記載のデータ記録再生システム。

【請求項6】 前記受信手段と、前記暗号化手段と、前記暗号解読手段とは、チューナ装置に備えられ、前記記録手段と、前記再生手段とは、VTR装置に備えられていることを特徴とする請求項4に記載のデータ記録再生システム。

【請求項7】 前記第2の暗号化は、公開鍵を用いて施され、前記暗号化ワークキーの解読は、前記公開鍵に対応する秘密鍵を用いて施されることを特徴とする請求項6に記載のデータ記録再生システム。

【請求項8】 前記鍵復元手段は、前記チューナ装置に備えられていることを特徴とする請求項7に記載のデータ記録再生システム。

【請求項9】 前記公開鍵および前記秘密鍵は、前記チューナ装置に対して固有な鍵であることを特徴とする請求項8に記載のデータ記録再生システム。

【請求項10】 前記公開鍵および前記秘密鍵は、前記チューナ装置の機器モデルに対して固有な鍵であること

を特徴とする請求項8に記載のデータ記録再生システム。

【請求項11】 前記チューナ装置は、ICカードに記録された情報を読み取るカード読取手段を有することを特徴とする請求項8に記載のデータ記録再生システム。

【請求項12】 前記公開鍵および前記秘密鍵は、前記ICカードに記録されたユーザIDに対して固有な鍵であることを特徴とする請求項11に記載のデータ記録再生システム。

【請求項13】 前記ICカードには、前記ユーザIDに対して固有な鍵に加えて、少なくとも一つの別のユーザIDに対して固有な公開鍵が記録されており、前記鍵暗号化手段は、前記第2の暗号化とともに、前記別のユーザIDに対して固有な公開鍵を用いて、前記ワークキーを暗号化して、前記別のユーザIDに対して固有な公開鍵毎に、別の暗号化ワークキーを生成し、前記記録手段は、前記暗号化ワークキーに加えて、前記別の暗号化ワークキーも前記記録媒体に記録することを特徴とする請求項12に記載のデータ記録再生システム。

【請求項14】 前記公開鍵および前記秘密鍵は、前記ICカードに記録されたサービスに対して固有な鍵であることを特徴とする請求項11に記載のデータ記録再生システム。

【請求項15】 前記鍵暗号化手段は、前記チューナ装置または前記VTR装置のいずれかに備えられていることを特徴とする請求項8～14のいずれかに記載のデータ記録再生システム。

【請求項16】 前記鍵暗号化手段が前記VTR装置に備えられている場合は、前記チューナ装置は、前記ワークキーを共通鍵によって暗号化する第二の鍵暗号化手段を有し、前記VTR装置は、前記共通鍵によって暗号化された前記ワークキーを解読する第二の鍵復元手段を有することを特徴とする請求項15に記載のデータ記録再生システム。

【請求項17】 前記公開鍵および前記秘密鍵は、前記VTR装置に対して固有な鍵であり、前記鍵暗号化手段および前記鍵復元手段は、前記VTR装置に備えられていることを特徴とする請求項7に記載のデータ記録再生システム。

【請求項18】 前記チューナ装置は、前記ワークキーを共通鍵によって暗号化する第二の鍵暗号化手段と、前記共通鍵によって暗号化された前記ワークキーを解読する第二の鍵復元手段とを有し、前記VTR装置は、前記ワークキーを前記共通鍵によって暗号化する第三の鍵暗号化手段と、前記共通鍵によって暗号化された前記ワークキーを解読する第三の鍵復元手段とを有し、前記第三の鍵復元手段は、前記第二の鍵暗号化手段により暗号化された前記ワークキーを解読し、前記第二の鍵復元手段は、前記第三の鍵暗号化手段により暗号化された前記ワークキーを解読することを特徴とする請求項17に記載

のデータ記録再生システム。

【請求項19】 前記第2の暗号化および前記暗号化ワークキーの解読は、共通鍵を用いて施され、前記鍵暗号化手段および前記鍵復元手段は、前記チューナ装置に備えられていることを特徴とする請求項6に記載のデータ記録再生システム。

【請求項20】 前記共通鍵は、前記チューナ装置、もしくは、前記チューナ装置の機器モデルに対して固有な鍵であることを特徴とする請求項19に記載のデータ記録再生システム。

【請求項21】 前記チューナ装置は、ICカードに記録された情報を読み取るカード読取手段を有し、前記共通鍵は、前記ICカードに記録されたユーザID、もしくは、前記ICカードに記録されたサービスに対して固有な鍵に対して固有な鍵であることを特徴とする請求項19に記載のデータ記録再生システム。

【請求項22】 前記チューナ装置は、前記記録媒体の記録時に課金情報を生成し、それを記憶することを特徴とする請求項6～21のいずれかに記載のデータ記録再生システム。

【請求項23】 前記チューナ装置は、前記記録媒体の再生時に課金情報を生成し、それを記憶することを特徴とする請求項6～21のいずれかに記載のデータ記録再生システム。

【請求項24】 前記記録媒体の記録時に、前記課金情報を生成するために必要な情報を、前記記録媒体に記録し、前記記録媒体の再生時に前記必要な情報を用いて前記課金情報を生成することを特徴とする請求項23に記載のデータ記録再生システム。

【請求項25】 前記課金情報は、前記記録媒体の再生期間の限定を伴うものであることを特徴とする請求項23または24に記載のデータ記録再生システム。

【請求項26】 前記課金情報は、前記記録媒体の再生回数の限定を伴うものであることを特徴とする請求項23～25のいずれかに記載のデータ記録再生システム。

【請求項27】 前記チューナ装置は、前記ICカードに前記課金情報を記憶させることを特徴とする請求項22～26のいずれかに記載のデータ記録再生システム。

【請求項28】 前記チューナ装置は、前記課金情報をサービスプロバイダに対して、通信を介して、出力することを特徴とする請求項22～27のいずれかに記載のデータ記録再生システム。

【請求項29】 前記暗号化ワークキーを、前記記録媒体の外部に出力されないデータ領域に記録することを特徴とする請求項4～28のいずれかに記載のデータ記録再生システム。

【請求項30】 前記第2の暗号化を施した鍵の固有性に関する情報を、前記記録媒体に記録することを特徴とする請求項4～29のいずれかに記載のデータ記録再生システム。

【請求項31】 前記ワークキーを、定期的または不定期的に切り替えることを特徴とする請求項4～30のいずれかに記載のデータ記録再生システム。

【請求項32】 前記切り替えの後のワークキーに対応する前記暗号化ワークキーが、前記切り替えの前のワークキーに対応する前記暗号化デジタルデータの少なくとも一部とタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項31に記載のデータ記録再生システム。

【請求項33】 一つの前記ワークキーに対応する前記暗号化ワークキーが、それに対応する前記暗号化デジタルデータとタイミング的に重なるように、前記記録媒体は再生されることを特徴とする請求項31または32に記載のデータ記録再生システム。

【請求項34】 前記チューナ装置を備える場合は、前記チューナ装置が前記切り替えを行うことを特徴とする請求項31～33のいずれかに記載のデータ記録再生システム。

【請求項35】 前記VTR装置を備える場合は、前記VTR装置が、前記切り替えに対応して、前記暗号化ワークキーの再生のタイミングを決定することを特徴とする請求項31～34のいずれかに記載のデータ記録再生システム。

【請求項36】 前記暗号化デジタルデータおよび前記暗号化ワークキーは、前記記録媒体上の前記再生のタイミングに対応する記録位置に、記録されることを特徴とする請求項31～35のいずれかに記載のデータ記録再生システム。

【請求項37】 前記切り替えのタイミングも合わせて、前記記録媒体に記録することを特徴とする請求項36に記載のデータ記録再生システム。

【請求項38】 前記チューナ装置および前記VTR装置を備える場合は、前記VTR装置が、前記切り替えの後のワークキー、もしくは、それに対応する前記暗号化ワークキーを、前記切り替えの後のワークキーに対応する前記暗号化デジタルデータの出力より前もって、前記チューナ装置へ出力することを特徴とする請求項31～37のいずれかに記載のデータ記録再生システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、データ記録再生方法およびデータ記録再生システムに関するものである。

【0002】

【従来の技術】衛星放送の録画、再生をユーザーが自由に行え、少数のユーザーを介して、不特定多数の者に、録画された番組が無制限に供給されることが可能になるため、この対策を講ずることは、プロバイダにとって必要不可欠なことである。

【0003】以下に、従来の衛星放送の記録再生方法を、図26を参照して説明する。図26は、従来の衛星

放送のデータ記録再生システムを示す構成図である。本システムは、衛星からの電波を受信するアンテナ903、ICカード902に記録された情報に基づいて、受信した電波をAVデータに変換するSTB(Set Top Box; 衛星放送受信機)901、前記AVデータを映像出力するモニター904、前記AVデータを記録媒体906に記録/再生するVTR装置905から構成されている。

【0004】まず、希望の番組を視聴する場合の手順について説明する。ユーザーが視聴希望の番組を選択すると、その番組の視聴料金に対応する視聴用課金情報が、ICカード902に記録される。原則として各番組のAVデータには、スクランブルがかけられており、当該番組の視聴用課金情報が、ICカード902に記録されている場合のみ、STB901がスクランブルを解除して、スクランブルがない状態でモニター904が映像出力する。ただし、STB901がスクランブルを解除しても、当該AVデータにはコピー防止信号(マクロビジョン)がかかっているため、この状態で、記録媒体に記録しても、再生時の再生画像が乱れてしまう。

【0005】次に、希望の番組を録画/再生する場合の手順について説明する。ユーザーが録画希望の番組を選択すると、その番組の録画料金に対応する録画用課金情報が、ICカード902に記録される。当該番組の録画用課金情報が、ICカード902に記録されている場合のみ、STB901が前述したマクロビジョンを解除して、乱れのないAVデータをVTR装置905に出力し、VTR装置905は、これを記録媒体906に記録する。記録されたAVデータは、マクロビジョンがかかっていないため、通常のAVデータと同様の再生方法で、映像出力が得られる。

【0006】以上の手順で、ICカード902に記録された視聴用課金情報および録画用課金情報は、一定期間分が電話回線等によって、プロバイダに通知される。

【0007】なお、図26では、STB装置とVTR装置が分離したタイプの衛星放送のデータ記録再生システムについて説明したが、各装置の機能を一つの装置に集約したタイプのものもある。

【0008】

【発明が解決しようとする課題】しかしながら、上述した記録再生方法では、一度課金されて記録された記録媒体は、以後の課金無しで、何回でも再生でき、また、当該記録媒体を複製することも容易に行えるという問題点がある。

【0009】上記問題点の対策として、AVデータが記録された記録媒体に、当該AVデータ記録時に使用したSTBおよび/またはVTR装置のIDも記録しておき、IDが異なる機器で再生しようとする、再生できないようにするという方法が提案されている。しかし、ID識別機能を有しない機器を用いる場合は、IDの一

致に関わりなく再生が可能であるという課題がある。また、全ての機器がID識別機能を有するとの前提に立てば、機器固有のIDを用いているために、当該機器が修復不可能な故障・破損等によって、使用できなくなった場合には、当該記録媒体に記録されたAVデータは、再生が不可能になってしまうという課題がある。

【0010】本発明は、上述した従来のデータ記録再生方法の課題を考慮し、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供することを第一の目的とするものである。また、前記第一の目的に加え、記録および/または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することを目的とするものである。さらに、前記第一の目的に加え、再生時のロスタイムが少ないデータ記録再生システムを提供することを目的とするものである。

【0011】

【課題を解決するための手段】上述した課題を解決するために、請求項1の本発明は、デジタルデータにワークキーを用いて第1の暗号化を施した暗号化デジタルデータと、前記ワークキーに第2の暗号化を施した暗号化ワークキーとを記録媒体に記録し、記録された前記暗号化デジタルデータおよび前記暗号化ワークキーを再生し、前記暗号化ワークキーを解読して得られた前記ワークキーを用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得ることを特徴とするデータ記録再生方法である。

【0012】請求項4の本発明は、外部からデジタルデータを受信する受信手段と、ワークキーを生成し、前記デジタルデータに前記ワークキーを用いて第1の暗号化を施して暗号化デジタルデータを生成する暗号化手段と、前記ワークキーに第2の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段と、前記暗号化デジタルデータおよび前記暗号化ワークキーを記録媒体に記録する記録手段と、前記記録媒体から前記暗号化デジタルデータおよび前記暗号化ワークキーを再生する再生手段と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段と、復元された前記ワークキーを用いて前記暗号化デジタルデータを解読して、前記デジタルデータを得る暗号解読手段とを備えることを特徴とするデータ記録再生システムである。

【0013】請求項22の本発明は、前記チューナ装置は、前記記録媒体の記録時に課金情報を生成し、それを記憶することを特徴とする請求項6～21のいずれかに記載のデータ記録再生システムである。

【0014】請求項23の本発明は、前記チューナ装置は、前記記録媒体の再生時に課金情報を生成し、それを記憶することを特徴とする請求項6～21のいずれかに

記載のデータ記録再生システムである。

【0015】請求項30の本発明は、前記第2の暗号化を施した鍵の固有性に関する情報を、前記記録媒体に記録することを特徴とする請求項4〜29のいずれかに記載のデータ記録再生システムである。

【0016】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【0017】(第1の実施の形態)以下に、本発明の第1の実施の形態を図面を参照して説明する。

【0018】図1は、本発明の第1の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムは、本発明のチューナ装置に対応するSTB(Set Top Box; 衛星放送受信機)1と、STB1にユーザーID等の情報を与えるICカード2と、STB1に接続されているアンテナ3およびモニター4と、本発明のVTR装置に対応するVTR装置5と、VTR装置5によってデータを記録/再生される記録媒体6とから構成されている。

【0019】STB1は、ICカード2に記録された情報の読み取り、必要情報をICカード2に記録するカード読取手段10と、STB1の機器ID等の情報を記憶するSTB情報記憶手段11と、モニター4での出力画像に対してデコードされたAVデータを出力するデコーダ12と、ワークキーを生成し、AVデータに前記ワークキーを用いて暗号化を施して暗号化AVデータを生成する暗号化手段13と、前記ワークキーに第2の暗号化を施して暗号化ワークキーを生成する鍵暗号化手段15と、前記暗号化ワークキーを解読して前記ワークキーを復元する鍵復元手段16と、復元された前記ワークキーを用いて前記暗号化AVデータを解読して、前記AVデータを得る暗号解読手段14と、VTR装置5とのデータの伝達を行うVTR伝達手段17と、人工衛星からの電波をアンテナ3を介して受信して、STB1内部用の信号に変換する受信手段20とを備えている。また、VTR伝達手段17は、VTR装置5のSTB伝達手段50と直接データの伝達を行うD-I/F(デジタルインターフェイス)18およびVTR装置5のSTB伝達手段50と認証鍵の交換を行ってVTR装置5の確認を行う認証鍵交換部19を有しており、受信手段20は、アンテナ3と直結し、受信したデータの復調を行う受信復調部21と、受信したデータに施されている放送用暗号を解除する放送用暗号解除部22と、多重化されている受信データを分離するDMUX(De-multiplexer; 分離部)23とを有している。なお、STB1は、上記の他に、STB1の装置全体を制御するSTB制御手段(図示せず)を備えている。

【0020】VTR装置5は、STB1とのデータの伝達を行うSTB伝達手段50と、前記暗号化AVデータ

および前記暗号化ワークキーを記録媒体6に記録する記録手段53と、記録媒体6から前記暗号化AVデータおよび前記暗号化ワークキーを再生する再生手段56とを備えている。また、STB伝達手段50は、STB1のVTR伝達手段17と直接データの伝達を行うD-I/F(デジタルインターフェイス)51およびSTB1のVTR伝達手段17と認証鍵の交換を行ってSTB1の確認を行う認証鍵交換部52を有している。また、記録手段53は、前記暗号化AVデータおよび前記暗号化ワークキーに対して記録媒体6のフォーマットに適合した多重化を行うMUX(Multiplexer; 多重化部)54および多重化されたデータを記録媒体6に記録する記録処理部55を有しており、再生手段56は、記録媒体6に記録されたデータを再生する再生処理部58および多重化された再生データを分離するDMUX(De-multiplexer; 分離部)57とを有している。なお、VTR装置5は、上記の他に、VTR装置5の装置全体を制御するVTR制御手段(図示せず)を備えている。

【0021】次に、このような本実施の形態の動作を説明する。

【0022】まず、AVデータを記録媒体6に記録する時のデータの流れを図2を用いて説明する。図2は、本発明の第1の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図2において、図1で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、Dは、記録しようとするAVデータの生データを、Kwは、AVデータDの暗号化に用いるワークキーを、Kw(D)は、AVデータDにワークキーKwを用いて暗号化を施して得られる暗号化AVデータを、 $_{STB}Pa$ は、ワークキーKwの暗号化に用いるSTB1に固有の公開鍵を、 $_{STB}Pa(Kw)$ は、ワークキーKwに公開鍵 $_{STB}Pa$ を用いて暗号化を施して得られる暗号化ワークキーを、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、ワークキーKwを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【0023】放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調部21で復調され、放送用の暗号を放送用暗号解除部22で解除され、DMUX23で分離されて、生のAVデータDとなって、デコーダ12および暗号化手段13へ送られる。デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、モニター4へ出力する。暗号化手段13は、ワークキーKwを生成し、生成したワークキーKwを用いて、AVデータDに暗号化を施して、暗号化AVデータKw(D)を生成する。生成されたワークキーKwは、鍵暗号化手段15へ送ら

れ、鍵暗号化手段15は、STB情報記憶手段11に記憶されているSTB1に固有の公開鍵 $s_{TB}Pa$ を用いて、ワークキー Kw に暗号化を施して、暗号化ワークキー $s_{TB}Pa(Kw)$ を生成する。

【0024】暗号化AVデータ $Kw(D)$ は、 $D-I/F18$ を介して、暗号化ワークキー $s_{TB}Pa(Kw)$ は、認証鍵交換部19および $D-I/F18$ を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換部19、52は、 $D-I/F18$ および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0025】VTR装置5へ伝達された暗号化AVデータ $Kw(D)$ は、 $D-I/F51$ を介して、暗号化ワークキー $s_{TB}Pa(Kw)$ は、 $D-I/F51$ および認証鍵交換部52を介して、それぞれMUX54へ送られて、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理部55によって、記録媒体6に記録される。

【0026】次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを図3を用いて説明する。図3は、本発明の第1の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図3において、図1で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。 $s_{TB}Sa$ は、公開鍵 $s_{TB}Pa$ に対応し、暗号化ワークキー $s_{TB}Pa(Kw)$ を解読してワークキー Kw を復元するのに用いるSTB1に固有の秘密鍵を示す。図中の他の記号は、図2に倣う。

【0027】多重化されて記録媒体6に記録された暗号化AVデータ $Kw(D)$ および暗号化ワークキー $s_{TB}Pa(Kw)$ は、再生処理部58により再生され、DMUX57で分離される。

【0028】分離された暗号化AVデータ $Kw(D)$ は、 $D-I/F51$ を介して、分離された暗号化ワークキー $s_{TB}Pa(Kw)$ は、認証鍵交換部52および $D-I/F51$ を介して、それぞれSTB1へ伝達されるが、それに先だって、記録時と同様に、STB1、VTR装置5それぞれの認証鍵交換部19、52は、 $D-I/F18$ および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0029】STB1へ伝達された暗号化AVデータ $Kw(D)$ は、 $D-I/F18$ を介して、暗号解読手段14へ送られ、暗号化ワークキー $s_{TB}Pa(Kw)$ は、 $D-I/F18$ および認証鍵交換部19を介して、鍵復元手段16へ送られる。鍵復元手段16は、STB情報記憶手段11に記憶されているSTB1に固有の秘密鍵 $s_{TB}Sa$ を用いて、暗号化ワークキー $s_{TB}Pa(Kw)$ をワークキー Kw に復元して、暗号解読手段14へ送

る。暗号解読手段14は、復元されたワークキー Kw を用いて、暗号化AVデータ $Kw(D)$ を解読して得られるAVデータ D を、デコーダ12へ出力する。デコーダ12は、AVデータ D に施された高能率符号化処理等をデコードし、モニター4へ出力する。

【0030】以上の手順にしたがって、AVデータを記録/再生することにより、AVデータに暗号化を施すのに用いたワークキーにSTB1に固有の公開鍵を用いて暗号化を施して、暗号化されたAVデータと一緒に記録媒体に記録し、再生時には暗号化されたワークキーをSTB1に固有の秘密鍵を用いて復元しているため、STB1に固有の秘密鍵を持っているシステム、すなわち、STB1そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

【0031】次に、本実施の形態におけるデータ記録再生システムの課金方法について説明する。本課金方法は、AVデータの記録/再生時に課金するものであるため、図2、図3を参照して説明する。

【0032】まず、記録時の課金方法について説明する。図2において、STB1のSTB制御手段(図示せず)は、記録時に、課金情報を生成し、これをカード読取手段10を介して、ICカード2に記録させる。記録のタイミングとしては、例えば、ユーザーからの記録指令に連動して記録するとしてもよいし、暗号化手段13または鍵暗号化手段15の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容としては、課金の金額そのものを記録するものであってもよいし、課金内容を特定するための識別子のようなものであってもよい。

【0033】次に、再生時の課金方法について説明する。図3において、STB1のSTB制御手段(図示せず)は、再生時に、課金情報を生成し、これをカード読取手段10を介して、ICカード2に記録する。記録のタイミングとしては、例えば、ユーザーからの再生指令に連動して記録するとしてもよいし、暗号解読手段14または鍵復元手段16の最初の出力に連動して記録するとしてもよい。記録する課金情報の内容については、記録時と同様である。

【0034】ICカード2に記録された課金情報は、定期的または不定期に、衛星放送のサービスプロバイダに対して、電話回線等の通信を介して出力され、サービスプロバイダは、この課金情報に基づいて、ユーザーの銀行口座からの引き落とし等の方法によって、ユーザーから課金の徴収を行う。

【0035】なお、上記説明において、課金情報は記録時および再生時に記録する、すなわち、記録、再生の両方に対して課金を行うとして説明したが、これに限ら

ず、いずれか一方についてのみ、課金を行うとしてもよい。

【0036】また、課金情報は、カード読取手段10を介して、ICカード2に記録されるとして説明したが、これに限らず、例えば、STB情報記憶手段11に記録されるとしてもよい。なお、STB情報記憶手段11に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ICカード2およびカード読取手段10を省いてもよい。

【0037】また、再生時の課金情報は、再生期間の限定および／または再生回数の限定を伴っていてもよい。例えば、ある期間を過ぎる、またはある再生回数を超えると、課金の金額が変わるというものでよい。ただし、再生回数の限定を伴う場合には、再生する毎に、記録媒体6等に通算再生回数を示す情報を書き込む必要がある。

【0038】さらに、記録時に、再生時の課金情報を生成するために必要な情報を、記録媒体6に記録し、記録媒体6の再生時に前記必要な情報を用いて課金情報を生成するとしてもよい。このときは、例えば、STB制御手段が記録時に前記必要な情報を生成し、これを、VTR伝達手段17およびSTB伝達手段50を介して、記録手段53に送り、記録手段53は、記録データの最初にこれを記録する。再生時には、前記必要な情報は、再生手段56によって再生され、STB伝達手段50およびVTR伝達手段17を介して、STB制御手段へ送られ、STB制御手段は、これに基づいて、再生時の課金情報を生成する。

【0039】以上説明したところから、本実施の形態におけるデータ記録再生システムは、記録および／または再生時に、確実に課金が可能なデータ記録再生システムであることがわかる。

【0040】次に、本実施の形態におけるデータ記録再生システムによって、記録媒体に記録されるデータの、記録媒体上の記録領域について、図2、図4を参照して説明する。

【0041】図4は、本発明の第1の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。図4の左右方向は、記録媒体6の時間的な記録位置を示し、上下方向は、同時刻に記録されたデータの構成を示す。図4において、記録領域は、メインエリアとサブエリアとに分けられており、メインエリアには、暗号化AVデータと、ワークキー変更のタイミングを示すフラッグとが書き込まれており、サブエリアには、当該記録位置に対応するメインエリアの位置に記録された暗号化AVデータ(Kw-a(D)、Kw-b(D)、Kw-c(D)、Kw-d(D)、...)の暗号化に用いられたワークキー(Kw-a、Kw-b、Kw-c、Kw-d、...)に、公開鍵 $_{STB}Pa$ を用いて暗号化を施して得られた、暗号

化ワークキー($_{STB}Pa(Kw-a)$ 、 $_{STB}Pa(Kw-b)$ 、 $_{STB}Pa(Kw-c)$ 、 $_{STB}Pa(Kw-d)$ 、...)と、次のワークキーの切替後に用いられるワークキー(Kw-b、Kw-c、Kw-d、Kw-e、...)に、公開鍵 $_{STB}Pa$ を用いて暗号化を施して得られた、暗号化ワークキー($_{STB}Pa(Kw-b)$ 、 $_{STB}Pa(Kw-c)$ 、 $_{STB}Pa(Kw-d)$ 、 $_{STB}Pa(Kw-e)$ 、...)とが書き込まれている。ただし、図4中においては、暗号化ワークキー $_{STB}Pa(Kw-a)$ 、 $_{STB}Pa(Kw-b)$ 、 $_{STB}Pa(Kw-c)$ 、 $_{STB}Pa(Kw-d)$ 、...は、便宜上、暗号化前のワークキーKw-a、Kw-b、Kw-c、Kw-d、...で表現している。

【0042】前述したように、暗号化手段13は、ワークキーKwを定期的または不定期的に切り替えて生成し、生成したワークキーKwを用いて、AVデータDに暗号化を施して、暗号化AVデータKw(D)を生成するが、現在使用中のワークキー(例えば、Kw-a)の次の切替後のワークキー(例えば、Kw-b)をあらかじめ生成して、その使用に先立って、鍵暗号化手段15により暗号化ワークキー $_{STB}Pa(Kw-a)$ に変換して、認証鍵交換部19、D-I/F18、51を介して、MUX54へ送り、記録処理部55は、これを現在使用中のワークキーKw-a、それによって暗号化された暗号化AVデータKw-a(D)等とともに、図4に示した記録領域に記録する。なお、ワークキー変更のタイミングを示すフラッグは、例えば、AVデータを伝送するパケットヘッダに付加されて伝達されてくるものとし、記録処理部55は、これをもとに、各記録データの記録位置を決定する。

【0043】図4に示すように、切り替えの後のワークキー、例えば、Kw-b、に対応する暗号化ワークキー $_{STB}Pa(Kw-b)$ は、切り替えの前のワークキーKw-aに対応する暗号化AVデータKw-a(D)の少なくとも一部と重なるように、記録媒体6に記録されており、切り替えの前のワークキーKw-aは、それに対応する暗号化AVデータKw-a(D)が記録されている位置に重なって、記録媒体6に記録されている。なお、暗号化ワークキー $_{STB}Pa(Kw-b)$ の記録領域は、図4においては、その次のワークキーKw-cに対応する暗号化ワークキー $_{STB}Pa(Kw-c)$ が書き込まれる直前まで書き込まれているが、少なくとも暗号化ワークキー $_{STB}Pa(Kw-c)$ が書き込まれる前に書き込みが終了していればよい、すなわち、図4中の暗号化ワークキー $_{STB}Pa(Kw-b)$ の記録領域は、少なくとも暗号化AVデータKw-a(D)の一部と重なるように記録されておれば、暗号化ワークキー $_{STB}Pa(Kw-c)$ の記録領域の始端との間にデータの空白領域があってもよい。

【0044】以上の記録要領によって、記録媒体への記

録を行うことによって、再生時には、次のワークキーをあらかじめ解読できるので、本実施の形態におけるデータ記録再生システムは、再生時のロスタイムが少ないデータ記録再生システムであることがわかる。

【0045】なお、本発明の記録媒体上の記録領域への記録要領は、本実施の形態における上述した記録要領に限るものではなく、例えば、暗号化手段13が次の切替後のワークキーをあらかじめ生成せず、VTR装置5が、STB1から送られてくるデータを一時記憶する手段を有し、前記一時記憶する手段に現在のデータを一時記憶させて、ワークキー切替後のデータを受け取った後に、記録媒体6への記録領域を決定して、記録するとしてもよい。

【0046】また、上述した記録要領に加えて、ワークキーKwの暗号化に用いた鍵を特定できる情報を記録媒体6に記録するとしてもよい。具体的には、本実施の形態においては、STB1のID情報である。この情報を利用して、例えば、STB1以外のSTBを用いて再生をしようとした場合、当該STBでは再生できない旨の警告とともに、再生可能なSTB（ここではSTB1）のID情報を表示することができる。

【0047】また、暗号化ワークキーを記録媒体6中の外部に出力されないデータ領域に記録してもよい。例えば、D-VHSシステムであれば、サブコード領域に記録する。これによって、さらに、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムとなる。

【0048】さらに、本実施の形態においては、暗号化デジタルデータおよび暗号化ワークキーは、記録媒体上の再生のタイミングに対応する記録位置に記録されるとして説明したが、これに限るものではなく、記録位置にとらわれず、切り替えの後のワークキーに対応する暗号化ワークキーが、切り替えの前のワークキーに対応する暗号化デジタルデータの少なくとも一部とタイミング的に重なるように、また、一つのワークキーに対応する暗号化ワークキーが、それに対応する暗号化デジタルデータとタイミング的に重なるように、再生されさえすればよい。

【0049】なお、上述した本実施の形態の課金方法および/または記録媒体上の記録領域への記録要領の替わりに、従来のものを用いる場合においては、上述したそれぞれの効果は得られないものの、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法およびデータ記録再生システムを提供するという、本発明の第一の目的は満足するものである。

【0050】（第2の実施の形態）以下に、本発明の第2の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、ワークキーの暗号化/復元を行う公開鍵/秘密鍵が、本発明のチューナ装置の機器モデルに対して固有な鍵であることに

関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

【0051】本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

【0052】次に、このような本実施の形態の動作を説明する。

【0053】本実施の形態においては、ワークキーKwの暗号化にSTB1の機器モデルに固有の公開鍵 $_{STB}Pa$ を用い、ワークキーKwを復元するのにSTB1の機器モデルに固有の秘密鍵 $_{STB}Sa$ を用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。したがって、本実施の形態の動作は、図2、図3において、公開鍵 $_{STB}Pa$ 、秘密鍵 $_{STB}Sa$ および暗号化ワークキー $_{STB}Pa(Kw)$ を、それぞれ、公開鍵 $_{STB}Pa$ 、秘密鍵 $_{STB}Sa$ および暗号化ワークキー $_{STB}Pa(Kw)$ に置き換えたもので示されるので、詳細の説明は、図2、図3に倣うとして省略する。

【0054】以上の手順にしたがって、AVデータを記録/再生することにより、本実施の形態は、第1の実施の形態によって得られる効果に加え、図5に示すように、STB1と同じモデルであるSTB101を所有しているユーザー間での記録媒体6の貸し借りが可能となり、かつ、STB1が修復不可能な故障・破損等によって、使用できなくなった場合においても、同じ機器モデルのSTBに代替すれば、引き続き使用できるものであることがわかる。

【0055】（第3の実施の形態）以下に、本発明の第3の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、ワークキーの暗号化/復元を行う公開鍵/秘密鍵が、本発明のICカードに記録されたユーザーIDに対して固有な鍵であることに関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

【0056】本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

【0057】次に、このような本実施の形態の動作を説明する。図6は、本発明の第2の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図7は、本発明の第2の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図6、図7に示すとおり、本実施の形態においては、ワークキーKwの暗号化にICカード2に記録されたユーザーIDに対して固有の公開鍵 $_{USER}Pa$ を用い、ワークキーKwを復元するの

にユーザIDに対して固有の秘密鍵 $USER\ S_a$ を用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。

【0058】以上の手順にしたがって、AVデータを記録／再生することにより、本実施の形態は、第1の実施の形態によって得られる効果に加え、STB1が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のSTB（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、ICカード2と一緒に記録媒体6の貸し借りをすれば、他のユーザーの使用が可能となるものであることがわかる。

【0059】また、本実施の形態において、上述のようにワークキー K_w の暗号化にICカード2に記録されたユーザIDに対して固有の公開鍵 $USER\ P_a$ を用いて、暗号化ワークキー $USER\ P_a\ (K_w)$ を生成するとともに、同じくICカード2に記録された他のユーザIDに対して固有の公開鍵 $USER1\ P_a$ を用いて、暗号化ワークキー $USER1\ P_a\ (K_w)$ も生成して、暗号化ワークキー $USER\ P_a\ (K_w)$ とともに、記録媒体6に記録しておけば、ICカード2を貸し出さなくても、公開鍵 $USER1\ P_a$ に対応する秘密鍵 $USER1\ S_a$ を保持している特定のユーザーは、その $USER1\ S_a$ を用いて暗号化ワークキー $USER1\ P_a\ (K_w)$ を復元できるので、その特定のユーザーに対してのみ、記録媒体6の貸し出し使用が可能となる。なお、公開鍵 $USER1\ P_a$ は、単数に限るものではなく、公開鍵 $USER1\ P_a \sim USERn\ P_a$ と、複数個であってもよい。すなわち、ユーザーは、貸し出し使用をしたい他のユーザーが生じた場合には、所定の手続きを経て、ICカード2に、当該他のユーザーに対応する公開鍵 $USERn\ P_a$ を記録して貰うことによって、当該他のユーザーへの簡単な貸し出し使用が可能となるものである。

【0060】なお、上記動作からわかるように、本実施の形態においては、図1に示した第1の実施の形態におけるデータ記録再生システムの構成から、STB記憶手段11を省略したものであってもよい。

【0061】（第4の実施の形態）以下に、本発明の第4の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、ワークキーの暗号化／復元を行う公開鍵／秘密鍵が、本発明のICカードに記録されたサービスに対して固有な鍵である点に関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

【0062】本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

【0063】次に、このような本実施の形態の動作を説明する。

【0064】図8は、本発明の第4の実施の形態におけ

るデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図9は、本発明の第4の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図8、図9に示すとおり、本実施の形態においては、ワークキー K_w の暗号化にICカード2に記録されたサービスに対して固有の公開鍵 $SERV\ P_a$ を用い、ワークキー K_w を復元するのにSTB1の機器モデルに固有の秘密鍵 $SERV\ S_a$ を用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。ここで、サービスに対して固有の鍵とは、具体的には、特定の番組に対してのみ固有、特定のジャンルの番組に対してのみ固有、特定のチャンネル番組に対してのみ固有、特定の衛星放送のプロバイダに対してのみ固有の鍵等が挙げられる。

【0065】例えば、特定の番組の記録／再生に対して、前もって料金を支払うことにより、その番組に固有の公開鍵 $SERV\ P_a$ および秘密鍵 $SERV\ S_a$ をICカード2に記憶させてもらうことにより、前記特定の番組の記録／再生が可能となるものである。この場合、公開鍵 $SERV\ P_a$ および秘密鍵 $SERV\ S_a$ がICカード2に記憶されていない場合は、記録できなくなる措置をSTB1が有する必要がある。なお、公開鍵 $SERV\ P_a$ および秘密鍵 $SERV\ S_a$ が必要な特定の番組以外の番組に対しては、第1～第3の実施の形態のいずれかで用いた公開鍵および秘密鍵に切り替えて、これらを用いるという、併用も可能である。

【0066】以上の手順にしたがって、AVデータを記録／再生することにより、本実施の形態は、第1の実施の形態によって得られる効果に加え、STB1が修復不可能な故障・破損等によって、使用できなくなった場合においても、他のSTB（同じ機器モデルでなくても可）に代替すれば、引き続き使用でき、かつ、記録されたAVデータに対応する特定のサービスを享受することを許可された特定のユーザーに対してのみ、記録媒体6の貸し借り使用が可能となるものであることがわかる。

【0067】なお、上記動作からわかるように、本実施の形態においては、図1に示した第1の実施の形態におけるデータ記録再生システムの構成から、STB記憶手段11を省略したものであってもよい。

【0068】（第5の実施の形態）以下に、本発明の第5の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、本発明の鍵暗号化手段がVTR装置に備えられており、それに伴って、本発明のチューナ装置が、ワークキーを共通鍵によって暗号化する第二の鍵暗号化手段を有し、本発明のVTR装置が、前記共通鍵によって暗号化された前記ワークキーを解読する第二の鍵復元手段を有することに関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについ

ては、第1の実施の形態と同じとする。

【0069】図10は、本発明の第5の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第1の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段62が、STB1ではなく、VTR装置5に備えられており、それに伴い、STB1は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段31を有し、VTR装置5は、本発明の第二の鍵復元手段に対応する鍵復元手段61と、鍵復元手段61および鍵暗号化手段62が用いる共通鍵、公開鍵等の情報を記憶するVTR情報記憶手段71とを有している。また、STB情報記憶手段11は、第1の実施の形態において保持していた情報に加えて、鍵暗号化手段31がワークキーを暗号化するのに用いる共通鍵の情報を保持している。

【0070】なお、第1の実施の形態と同様に、課金情報が、例えば、STB情報記憶手段11に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ICカード2およびカード読取手段10を省いてもよい。

【0071】次に、このような本実施の形態の動作を説明する。

【0072】まず、AVデータを記録媒体6に記録する時のデータの流れを図11を用いて説明する。図11は、本発明の第5の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図11において、図10で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図2、図3に倣う。Kcは、ワークキーKwの暗号化に用いるSTB1およびVTR装置5に共通な共通鍵を、AVデータDの暗号化に用いるワークキーを、Kc(Kw)は、ワークキーKwに共通鍵Kcを用いて暗号化を施して得られる暗号化ワークキーを、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第1の実施の形態と同様に、ワークキーKwを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【0073】放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調部21で復調され、放送用の暗号を放送用暗号解除部22で解除され、DMUX23で分離されて、生のAVデータDとなつて、デコーダ12および暗号化手段13へ送られる。デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、モニター4へ出力する。暗号化手段13は、ワークキーKwを生成し、生成したワークキーKwを用いて、AVデータDに暗号化を施して、暗号化AVデータKw(D)を生成する。生

成されたワークキーKwは、鍵暗号化手段31へ送られ、鍵暗号化手段31は、STB情報記憶手段11に記憶されているSTB1およびVTR装置5に共通な共通鍵Kcを用いて、ワークキーKwに暗号化を施して、暗号化ワークキーKc(Kw)を生成する。

【0074】暗号化AVデータKw(D)は、D-I/F18を介して、暗号化ワークキーKc(Kw)は、認証鍵交換部19およびD-I/F18を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換部19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0075】VTR装置5へ伝達された暗号化AVデータKw(D)は、D-I/F51を介して、MUX54へ送られる。また、VTR装置5へ伝達された暗号化ワークキーKc(Kw)は、D-I/F51および認証鍵交換部52を介して、鍵復元手段61に送られる。鍵復元手段61は、VTR情報記憶手段71に記憶されている共通鍵Kcを用いて、暗号化ワークキーKc(Kw)をワークキーKwに復元して、鍵暗号化手段62に送る。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているSTB1に固有の公開鍵 $_{STB}Pa$ を用いて、ワークキーKwに暗号化を施して、暗号化ワークキー $_{STB}Pa(Kw)$ を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータKw(D)および暗号化ワークキー $_{STB}Pa(Kw)$ は、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理部55によって、記録媒体6に記録される。

【0076】次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを図12を用いて説明する。図12は、本発明の第5の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図12からわかるように、本実施の形態においては、記録された暗号化ワークキー $_{STB}Pa(Kw)$ は、VTR装置5内では復元されずに、STB1の鍵復元手段16へ送られ、ここで、STB情報記憶手段11に記憶されているSTB1に固有の秘密鍵 $_{STB}Sa$ を用いることによって、ワークキーKwに復元される。図1で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。すなわち、AVデータを再生する時のデータの流れは、第1の実施の形態の図3と同じになる。

【0077】以上の手順にしたがって、AVデータを記録/再生することにより、AVデータの記録時において、VTR装置5への送信側であるSTB1におけるワークキーの暗号化が、負担の軽い共通鍵による暗号化としているので、AVデータの暗号化およびワークキーの暗号化を平行しておこなうことにより負担が増大しているSTB1の負担を軽減できるので、本実施の形態にお

けるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第1の実施の形態におけるデータ記録再生システムと比較して、STB1およびVTR装置5の負担を平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。

【0078】なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、第1の実施の形態と同じく、本発明のチューナ装置(STB1)に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第2〜第4いずれかの実施の形態と同じく、本発明のチューナ装置(STB1)の機器モデルに対して固有な鍵、本発明のICカードに記録されたユーザIDに対して固有な鍵、本発明のICカードに記録されたサービスに対して固有な鍵であってもよい。

【0079】また、本発明の公開鍵の情報は、本実施の形態においては、VTR情報記憶手段71に記憶されているものとして説明したが、これに限るものではなく、例えば、記録を始める際に、STB1から送られてくるとしてもよい。

【0080】なお、本実施の形態におけるデータ記録再生システムから、図13に示すように、鍵暗号化手段31および鍵復元手段61を省略した構成も可能である。こうすれば、本発明のチューナ装置からVTR装置へのデータ送信において、ワークキーに暗号化を施さずに送信を行うことになる。このような構成は、後述する第8の実施の形態のように、STBおよびVTR装置の機能を一体化した一体化STBを備えるデータ記録再生システムに適用すると、特に有効である。以下に、図13の構成のデータ記録再生システムについて説明する。

【0081】図13の構成のデータ記録再生システムにおける、AVデータを記録媒体6に記録する時のデータの流れは、図14に示すようになる。図14において、図13で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図11、図12に倣う。

【0082】放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調部21で復調され、放送用の暗号を放送用暗号解除部22で解除され、DMUX23で分離されて、生のAVデータDとなって、デコーダ12および暗号化手段13へ送られる。デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、モニター4へ出力する。暗号化手段13は、ワークキーKwを生成し、生成したワークキーKwを用いて、AVデータDに暗号化を施して、暗号化AVデータKw(D)を生成する。

【0083】暗号化AVデータKw(D)は、D-I/F18を介して、ワークキーKwは、認証鍵交換部19およびD-I/F18を介して、それぞれVTR装置5

へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換部19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0084】VTR装置5へ伝達された暗号化AVデータKw(D)は、D-I/F51を介して、MUX54へ送られる。また、VTR装置5へ伝達されたワークキーKwは、D-I/F51および認証鍵交換部52を介して、鍵暗号化手段62に送られる。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているSTB1に固有の公開鍵 $_{STB}Pa$ を用いて、ワークキーKwに暗号化を施して、暗号化ワークキー $_{STB}Pa(Kw)$ を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータKw(D)および暗号化ワークキー $_{STB}Pa(Kw)$ は、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理部55によって、記録媒体6に記録される。

【0085】図13の構成のデータ記録再生システムにおける、データ再生時のデータの流れについては、図12で示したデータ再生時のデータの流れと同じである。したがって、以下の説明を省略する。

【0086】なお、STB情報記憶手段11およびVTR情報記憶手段71は、図10の構成において保持していた共通鍵の情報を保持している必要はない。

【0087】以上の手順にしたがって、AVデータを記録/再生することにより、AVデータの記録時において、VTR装置5への送信側であるSTB1がワークキーの暗号化を行わないので、AVデータの暗号化およびワークキーの暗号化を平行しておこなうことにより負担が増大しているSTB1の負担をさらに軽減できるので、図13の構成のデータ記録再生システムは、図10の構成のデータ記録再生システムと比較して、STB1およびVTR装置5の負担をさらに平滑化して、記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図10の構成のデータ記録再生システムと比較して、STB1からVTR装置5へのデータ送信についてのセキュリティは低下する。このような構成は、後述する第8の実施の形態のように、STBおよびVTR装置の機能を一体化した一体化STBを備えるデータ記録再生システムに適用すると、特に有効である。

【0088】(第6の実施の形態)以下に、本発明の第6の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、本発明の鍵暗号化手段および鍵復元手段がVTR装置に備えられており、ワークキーの暗号化/復元を行う公開鍵/秘密鍵が、本発明のVTR装置に対して固有な鍵であることに関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないもの

については、第1の実施の形態と同じとする。

【0089】図15は、本発明の第6の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第1の実施の形態におけるデータ記録再生システムの構成と異なるのは、本発明の鍵暗号化手段に対応する鍵暗号化手段62および本発明の鍵復元手段に対応する鍵復元手段64が、STB1ではなく、VTR装置5に備えられており、それに伴い、STB1は、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段31および本発明の第二の鍵復元手段に対応する鍵復元手段32を有し、VTR装置5は、本発明の第二の鍵暗号化手段に対応する鍵復元手段61と、本発明の第二の鍵暗号化手段に対応する鍵暗号化手段63と、鍵復元手段61、鍵暗号化手段62、鍵暗号化手段63および鍵復元手段64が用いる共通鍵、公開鍵等の情報を記憶するVTR情報記憶手段71とを有している。また、STB情報記憶手段11は、第1の実施の形態において保持していた情報に加えて、鍵暗号化手段31がワークキーを暗号化するのに用いる共通鍵の情報を保持している。

【0090】なお、第1の実施の形態と同様に、課金情報が、例えば、STB情報記憶手段11に記録される場合は、本実施の形態の構成におけるデータ記録再生システムから、ICカード2およびカード読取手段10を省いてもよい。

【0091】次に、このような本実施の形態の動作を説明する。

【0092】まず、AVデータを記録媒体6に記録する時のデータの流れを図14を用いて説明する。図16は、本発明の第6の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図16において、図15で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、新たに説明するもの以外は、図2、図3に倣う。Kcは、ワークキーKwの暗号化に用いるSTB1およびVTR装置5に共通な共通鍵を、Kc(Kw)は、ワークキーKwに共通鍵Kcを用いて暗号化を施して得られる暗号化ワークキーを、 $v_{TR}Pa$ は、ワークキーKwの暗号化に用いるVTR装置5に固有の公開鍵を、 $v_{TR}Pa(Kw)$ は、ワークキーKwに公開鍵 $v_{TR}Pa$ を用いて暗号化を施して得られる暗号化ワークキーを、それぞれ示す。なお、本実施の形態におけるデータ記録再生システムは、第1の実施の形態と同様に、ワークキーKwを、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【0093】放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調部21で復調され、放送用の暗号を放送用暗号解除

部22で解除され、DMUX23で分離されて、生のAVデータDとなって、デコード12および暗号化手段13へ送られる。デコード12は、AVデータDに施された高能率符号化処理等をデコードし、モニター4へ出力する。暗号化手段13は、ワークキーKwを生成し、生成したワークキーKwを用いて、AVデータDに暗号化を施して、暗号化AVデータKw(D)を生成する。生成されたワークキーKwは、鍵暗号化手段31へ送られ、鍵暗号化手段31は、STB情報記憶手段11に記憶されているSTB1およびVTR装置5に共通な共通鍵Kcを用いて、ワークキーKwに暗号化を施して、暗号化ワークキーKc(Kw)を生成する。

【0094】暗号化AVデータKw(D)は、D-I/F18を介して、暗号化ワークキー $_{STB}Pa(Kw)$ は、認証鍵交換部19およびD-I/F18を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換部19、52は、D-I/F18および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0095】VTR装置5へ伝達された暗号化AVデータKw(D)は、D-I/F51を介して、MUX54へ送られる。また、VTR装置5へ伝達された暗号化ワークキーKc(Kw)は、D-I/F51および認証鍵交換部52を介して、鍵復元手段61に送られる。鍵復元手段61は、VTR情報記憶手段71に記憶されている共通鍵Kcを用いて、暗号化ワークキーKc(Kw)をワークキーKwに復元して、鍵暗号化手段62に送る。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているVTR装置5に固有の公開鍵 $v_{TR}Pa$ を用いて、ワークキーKwに暗号化を施して、暗号化ワークキー $v_{TR}Pa(Kw)$ を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータKw(D)および暗号化ワークキー $v_{TR}Pa(Kw)$ は、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理部55によって、記録媒体6に記録される。

【0096】次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを図17を用いて説明する。図17は、本発明の第6の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図17において、図15で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。 $v_{TR}Sa$ は、公開鍵 $v_{TR}Pa$ に対応し、暗号化ワークキー $v_{TR}Pa(Kw)$ を解読してワークキーKwを復元するのに用いるVTR装置5に固有の秘密鍵を示す。図中の他の記号は、図16に倣う。

【0097】多重化されて記録媒体6に記録された暗号化AVデータKw(D)および暗号化ワークキー $v_{TR}Pa(Kw)$ は、再生処理部58により再生され、DMU

X57で分離される。分離された暗号化ワークキー $v_{TR}Pa(Kw)$ は、鍵復元手段64へ送られる。鍵復元手段64は、VTR情報記憶手段71に記憶されているVTR装置5に固有の秘密鍵 $v_{TR}Sa$ を用いて、暗号化ワークキー $v_{TR}Pa(Kw)$ をワークキー Kw に復元して、鍵暗号化手段63へ送る。鍵暗号化手段63は、VTR情報記憶手段71に記憶されている共通鍵 Kc を用いて、ワークキー Kw に暗号化を施して、暗号化ワークキー $Kc(Kw)$ を生成する。

【0098】分離された暗号化AVデータ $Kw(D)$ は、 $D-I/F51$ を介して、生成された暗号化ワークキー $Kc(Kw)$ は、認証鍵交換部52および $D-I/F51$ を介して、それぞれSTB1へ伝達されるが、それに先だって、記録時と同様に、STB1、VTR装置5それぞれの認証鍵交換部19、52は、 $D-I/F18$ および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0099】STB1へ伝達された暗号化AVデータ $Kw(D)$ は、 $D-I/F18$ を介して、暗号解読手段14へ送られ、暗号化ワークキー $Kc(Kw)$ は、 $D-I/F18$ および認証鍵交換部19を介して、鍵復元手段32へ送られる。鍵復元手段32は、STB情報記憶手段11に記憶されている共通鍵 Kc を用いて、暗号化ワークキー $Kc(Kw)$ をワークキー Kw に復元して、暗号解読手段14へ送る。暗号解読手段14は、復元されたワークキー Kw を用いて、暗号化AVデータ $Kw(D)$ を解読して得られるAVデータ D を、デコーダ12へ出力する。デコーダ12は、AVデータ D に施された高能率符号化処理等をデコードし、モニター4へ出力する。

【0100】以上の手順にしたがって、AVデータを記録/再生することにより、AVデータに暗号化を施すのに用いたワークキーにVTR装置5に固有の公開鍵を用いて暗号化を施して、暗号化されたAVデータと一緒に記録媒体に記録し、再生時には暗号化されたワークキーをVTR装置5に固有の秘密鍵を用いて復元しているため、VTR装置5に固有の秘密鍵を持っているシステム、すなわち、VTR装置5そのものを備えているシステムしか再生できないので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであることがわかる。

【0101】なお、本実施の形態におけるデータ記録再生システムから、図18に示すように、鍵暗号化手段31、鍵復元手段32、鍵復元手段61および鍵暗号化手段63を省略した構成も可能である。こうすれば、本発明のチューナ装置とVTR装置との間のデータ送信において、ワークキーに暗号化を施さずに送信を行うことになる。以下に、図13の構成のデータ記録再生システム

について説明する。

【0102】図18の構成のデータ記録再生システムにおける、AVデータを記録媒体6に記録する時のデータの流れは、図19に示すようになる。図19において、図18で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図16、図17に倣う。

【0103】放送用電波として暗号化され、多重化されたAVデータ D は、アンテナ3を介して受信され、受信復調部21で復調され、放送用の暗号を放送用暗号解除部22で解除され、DMUX23で分離されて、生のAVデータ D となって、デコーダ12および暗号化手段13へ送られる。デコーダ12は、AVデータ D に施された高能率符号化処理等をデコードし、モニター4へ出力する。暗号化手段13は、ワークキー Kw を生成し、生成したワークキー Kw を用いて、AVデータ D に暗号化を施して、暗号化AVデータ $Kw(D)$ を生成する。

【0104】暗号化AVデータ $Kw(D)$ は、 $D-I/F18$ を介して、ワークキー Kw は、認証鍵交換部19および $D-I/F18$ を介して、それぞれVTR装置5へ伝達されるが、それに先だって、STB1、VTR装置5それぞれの認証鍵交換部19、52は、 $D-I/F18$ および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0105】VTR装置5へ伝達された暗号化AVデータ $Kw(D)$ は、 $D-I/F51$ を介して、MUX54へ送られる。また、VTR装置5へ伝達されたワークキー Kw は、 $D-I/F51$ および認証鍵交換部52を介して、鍵暗号化手段62に送られる。鍵暗号化手段62は、VTR情報記憶手段71に記憶されているVTR装置5に固有の公開鍵 $v_{TR}Pa$ を用いて、ワークキー Kw に暗号化を施して、暗号化ワークキー $v_{TR}Pa(Kw)$ を生成して、これをMUX54へ送る。MUX54へ送られた暗号化AVデータ $Kw(D)$ および暗号化ワークキー $v_{TR}Pa(Kw)$ は、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理部55によって、記録媒体6に記録される。

【0106】次に、図18の構成のデータ記録再生システムにおける、記録媒体6に記録されたAVデータを再生する時のデータの流れを図20を用いて説明する。図20において、図18で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。また、図中の記号については、図16、図17に倣う。

【0107】多重化されて記録媒体6に記録された暗号化AVデータ $Kw(D)$ および暗号化ワークキー $v_{TR}Pa(Kw)$ は、再生処理部58により再生され、DMUX57で分離される。分離された暗号化ワークキー $v_{TR}Pa(Kw)$ は、鍵復元手段64へ送られる。鍵復元手段64は、VTR情報記憶手段71に記憶されているV

TR装置5に固有の秘密鍵 $v_{TR}Sa$ を用いて、暗号化ワークキー $v_{TR}Pa(Kw)$ をワークキー Kw に復元する。

【0108】分離された暗号化AVデータ $Kw(D)$ は、 $D-I/F51$ を介して、復元されたワークキー Kw は、認証鍵交換部52および $D-I/F51$ を介して、それぞれSTB1へ伝達されるが、それに先だって、記録時と同様に、STB1、VTR装置5それぞれの認証鍵交換部19、52は、 $D-I/F18$ および51を介して、お互いの認証鍵を交換し、伝達可能な相手であることを確認した上で、前記伝達が行われる。

【0109】STB1へ伝達された暗号化AVデータ $Kw(D)$ は、 $D-I/F18$ を介して、暗号解読手段14へ送られ、ワークキー Kw は、 $D-I/F18$ および認証鍵交換部19を介して、それぞれ暗号解読手段14へ送られる。暗号解読手段14は、ワークキー Kw を用いて、暗号化AVデータ $Kw(D)$ を解読して得られるAVデータ D を、デコーダ12へ出力する。デコーダ12は、AVデータ D に施された高能率符号化処理等をデコードし、モニター4へ出力する。

【0110】なお、STB情報記憶手段11およびVTR情報記憶手段71は、図15の構成において保持していた共通鍵の情報を保持している必要はない。

【0111】以上の手順にしたがって、AVデータを記録/再生することにより、STB1とVTR装置5との間のデータ送信において、ワークキーに暗号化を施さずに送信を行うので、記録/再生時のSTB1およびVTR装置5の負担をさらに軽減できるので、図18の構成のデータ記録再生システムは、図15の構成のデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。ただし、図15の構成のデータ記録再生システムと比較して、STB1とVTR装置5との間のデータ送信についてのセキュリティは低下する。このような構成は、後述する第8の実施の形態のように、STBおよびVTR装置の機能を一体化した一体化STBを備えるデータ記録再生システムに適用すると、特に有効である。

【0112】(第7の実施の形態)以下に、本発明の第7の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、公開鍵および秘密鍵を用いる替わりに、共通鍵を用いてワークキーの暗号化/復元を行う点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

【0113】本実施の形態におけるデータ記録再生システムの構成は、第1の実施の形態におけるデータ記録再生システムの構成と同じである。

【0114】次に、このような本実施の形態の動作を説

明する。

【0115】図21は、本発明の第7の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図であり、図22は、本発明の第7の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図21、図22に示すとおり、本実施の形態においては、ワークキー Kw の暗号化および復元にSTB情報記憶手段11に保持されている共通鍵 Kc を用いている点以外は、第1の実施の形態におけるデータ記録再生システムと同じである。なお、共通鍵 Kc は、例えば、STB1もしくはSTB1の機器モデル、ユーザID、サービスいずれかに対して固有な鍵である。また、共通鍵 Kc は、ICカード2に記録されているとしてもよい。共通鍵 Kc がICカード2に記録されていない場合で、課金情報が、例えば、STB情報記憶手段11に記録される場合は、カード読取手段10を省略してもよい。また、共通鍵 Kc がSTB記憶手段11に記録されていない場合は、STB記憶手段11を省略してもよい。

【0116】以上の手順にしたがって、AVデータを記録/再生することにより、ワークキーに暗号化に公開鍵を用いないので、本実施の形態におけるデータ記録再生システムは、第1の実施の形態におけるデータ記録再生システムと比較して、鍵自身のデータ長を短くでき、記録効率の向上および装置の小型化を図ることが可能なシステムであることがわかる。

【0117】(第8の実施の形態)以下に、本発明の第8の実施の形態を図面を参照して説明する。本実施の形態が上述した第1の実施の形態と異なる点は、第1の実施の形態におけるデータ記録再生システムが本発明のチューナ装置およびVTR装置を備えていたのに対し、本実施の形態におけるデータ記録再生システムが前記チューナ装置および前記VTR装置の機能が一体化された装置を備えている点に関する点である。したがって、本実施の形態において、第1の実施の形態と同様の物については、同一符号を付与し、説明を省略する。また、特に説明のないものについては、第1の実施の形態と同じとする。

【0118】図23は、本発明の第8の実施の形態におけるデータ記録再生システムの構成を示す構成図である。本実施の形態におけるデータ記録再生システムの構成が、第1の実施の形態におけるデータ記録再生システムの構成と異なるのは、STB1およびVTR装置5の機能を一体化した一体化STB7を備えることによって、第1の実施の形態におけるデータ記録再生システムが備えていたVTR伝達手段17およびSTB伝達手段50を省略したことである。

【0119】なお、第1の実施の形態と同様に、課金情報が、例えば、STB情報記憶手段11に記録される場合は、本実施の形態の構成におけるデータ記録再生シス

テムから、ICカード2およびカード読取手段10を省いてもよい。

【0120】次に、このような本実施の形態の動作を説明する。

【0121】まず、AVデータを記録媒体6に記録する時のデータの流れを図24を用いて説明する。図24は、本発明の第8の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。図24において、図23で示した構成のうち、記録時に不要な手段等は、適宜省略して示す。また、図中の記号については、図2、図3に倣うが、 $STB Pa$ は、ワークキー Kw の暗号化に用いる一体化STB7に固有の公開鍵を示す。なお、本実施の形態におけるデータ記録再生システムは、第1の実施の形態と同様に、ワークキー Kw を、定期的または不定期的に切り替えることによって、切り替えない場合に比して、さらに、暗号化に関する情報が外部に漏洩しにくいシステムとなっている。

【0122】放送用電波として暗号化され、多重化されたAVデータDは、アンテナ3を介して受信され、受信復調部21で復調され、放送用の暗号を放送用暗号解除部22で解除され、DMUX23で分離されて、生のAVデータDとなって、デコーダ12および暗号化手段13へ送られる。デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、モニター4へ出力する。暗号化手段13は、ワークキー Kw を生成し、生成したワークキー Kw を用いて、AVデータDに暗号化を施して、暗号化AVデータ $Kw(D)$ を生成する。生成されたワークキー Kw は、鍵暗号化手段15へ送られ、鍵暗号化手段15は、STB情報記憶手段11に記憶されている一体化STB7に固有の公開鍵 $STB Pa$ を用いて、ワークキー Kw に暗号化を施して、暗号化ワークキー $STB Pa(Kw)$ を生成する。

【0123】生成された暗号化AVデータ $Kw(D)$ および暗号化ワークキー $STB Pa(Kw)$ は、それぞれMUX54へ送られて、記録媒体6のフォーマットに適合した多重化を行われた後、記録処理部55によって、記録媒体6に記録される。

【0124】次に、記録媒体6に記録されたAVデータを再生する時のデータの流れを図25を用いて説明する。図25は、本発明の第8の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。図25において、図23で示した構成のうち、再生時に不要な手段等は、適宜省略して示す。図中の記号は、図2、図3に倣うが、 $STB Sa$ は、公開鍵 $STB Pa$ に対応し、暗号化ワークキー $STB Pa(Kw)$ を解読してワークキー Kw を復元するのに用いる一体化STB7に固有の秘密鍵を示す。

【0125】多重化されて記録媒体6に記録された暗号化AVデータ $Kw(D)$ および暗号化ワークキー $STB Pa$

$a(Kw)$ は、再生処理部58により再生され、DMUX57で分離される。

【0126】分離された暗号化AVデータ $Kw(D)$ は、暗号解読手段14へ送られ、分離された暗号化ワークキー $STB Pa(Kw)$ は、鍵復元手段16へ送られる。鍵復元手段16は、STB情報記憶手段11に記憶されている一体化STB7に固有の秘密鍵 $STB Sa$ を用いて、暗号化ワークキー $STB Pa(Kw)$ をワークキー Kw に復元して、暗号解読手段14へ送る。暗号解読手段14は、復元されたワークキー Kw を用いて、暗号化AVデータ $Kw(D)$ を解読して得られるAVデータDを、デコーダ12へ出力する。デコーダ12は、AVデータDに施された高能率符号化処理等をデコードし、モニター4へ出力する。

【0127】以上の手順にしたがって、AVデータを記録／再生することにより、各装置間のデータ伝達にかかる負担を省略できるので、本実施の形態におけるデータ記録再生システムは、特定の対象に対してのみ、再生が可能であり、暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムであり、かつ、第1の実施の形態におけるデータ記録再生システムと比較して、さらに記録効率の向上を図ることが可能なシステムであることがわかる。なお、本発明の公開鍵および秘密鍵は、本実施の形態においては、一体化STB7に対して固有な鍵であるとして説明したが、これに限るものではなく、例えば、第2～第4いずれかの実施の形態と同様に、一体化STB7の機器モデルに対して固有な鍵、本発明のICカードに記録されたユーザIDに対して固有な鍵、本発明のICカードに記録されたサービスに対して固有な鍵であってもよい。

【0128】なお、本発明のワークキーは、上述した第1～第8の実施の形態においては、定期的または不定期的に切り替えられるとして説明したが、同じワークキーを用いるとすると、定期的または不定期的に切り替える場合と比較して、暗号化に関する情報が外部に漏洩するおそれが高くなるが、従来のデータ記録再生システムと比較すると、暗号化に関する情報が外部に漏洩しにくいシステムであるといえる。

【0129】また、本発明の第2の暗号化は、上述した第1～第8の実施の形態においては、本発明の第1の暗号化において用いたワークキーとは別の鍵（公開鍵、共通鍵）であるとして説明したが、これに限るものではなく、第1の暗号化に用いたワークキーに対応するアルゴリズムと同じアルゴリズムを用いて、当該ワークキー自身に第2の暗号化を施すとしてもよい。また、例えば、ワークキーとして共通鍵を用いてデジタルデータに第1の暗号化を施し、当該共通鍵に同じ共通鍵を用いて第2の暗号化を施すとしてもよい。

【0130】なお、上述した第1～第8の実施の形態においては、本発明のデータ記録再生システムを中心に説

明したが、本発明のデータ記録再生方法は、上記説明中で、説明された方法である。

【0131】

【発明の効果】以上説明したところから明らかなように、請求項1の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生方法を提供することができる。また、請求項4の本発明は、データに暗号化を施すことによって、特定の対象に対してのみ、再生が可能であり、前記暗号化に関する情報が外部に漏洩しにくいデータ記録再生システムを提供することができる。また、請求項22または23の本発明は、記録および/または再生時に、確実に課金が可能なデータ記録再生方法およびデータ記録再生システムを提供することができる。さらに、請求項30の本発明は、再生時のロスタイムが少ないデータ記録再生システムを提供することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図2】本発明の第1の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図3】本発明の第1の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図4】本発明の第1の実施の形態におけるデータ記録再生システムを用いて記録された記録媒体上の記録領域を示す模式図である。

【図5】本発明の第2の実施の形態におけるデータ記録再生システムで記録された記録媒体の貸与時の流れを示すフロー図である。

【図6】本発明の第3の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図7】本発明の第3の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図8】本発明の第4の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図9】本発明の第4の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図10】本発明の第5の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図11】本発明の第5の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図12】本発明の第5の実施の形態におけるデータ記

録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図13】本発明の第5の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

【図14】本発明の第5の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図15】本発明の第6の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図16】本発明の第6の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図17】本発明の第6の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図18】本発明の第6の実施の形態における別のデータ記録再生システムの構成を示す構成図である。

【図19】本発明の第6の実施の形態における別のデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図20】本発明の第6の実施の形態における別のデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図21】本発明の第7の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図22】本発明の第7の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

【図23】本発明の第8の実施の形態におけるデータ記録再生システムの構成を示す構成図である。

【図24】本発明の第8の実施の形態におけるデータ記録再生システムのデータ記録時のデータの流れを示すフロー図である。

【図25】本発明の第8の実施の形態におけるデータ記録再生システムのデータ再生時のデータの流れを示すフロー図である。

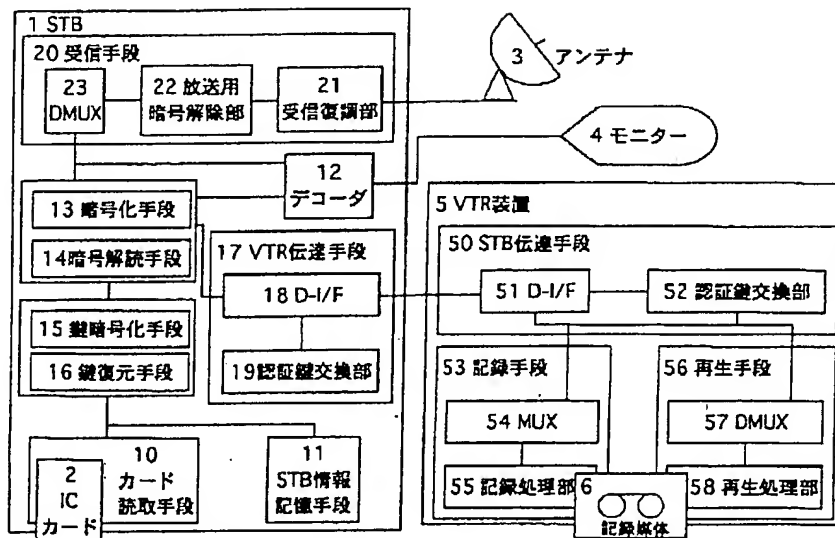
【図26】従来の衛星放送のデータ記録再生システムを示す構成図である。

【符号の説明】

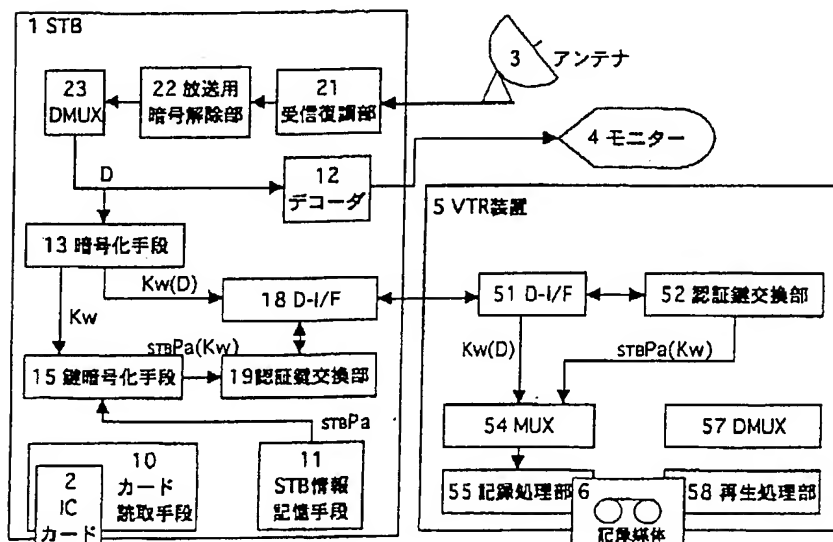
- 1、101、901 STB
- 2、102、902 ICカード
- 3、903 アンテナ
- 4、904 モニター
- 5、105、905 VTR装置
- 6、906 記録媒体
- 7 一体化STB
- 10 カード読取手段
- 11 STB情報記憶手段
- 12 デコーダ

- | | |
|--------------------|-------------|
| 13 暗号化手段 | 22 放送用暗号解除部 |
| 14 暗号解読手段 | 23、57 DMUX |
| 15、31、62、63 鍵暗号化手段 | 50 STB伝達手段 |
| 16、32、61、64 鍵復元手段 | 53 記録手段 |
| 17 VTR伝達手段 | 54 MUX |
| 18、51 D-I/F | 55 記録処理部 |
| 19、52 認証鍵交換部 | 56 再生手段 |
| 20 受信手段 | 58 再生処理部 |
| 21 受信復調部 | |

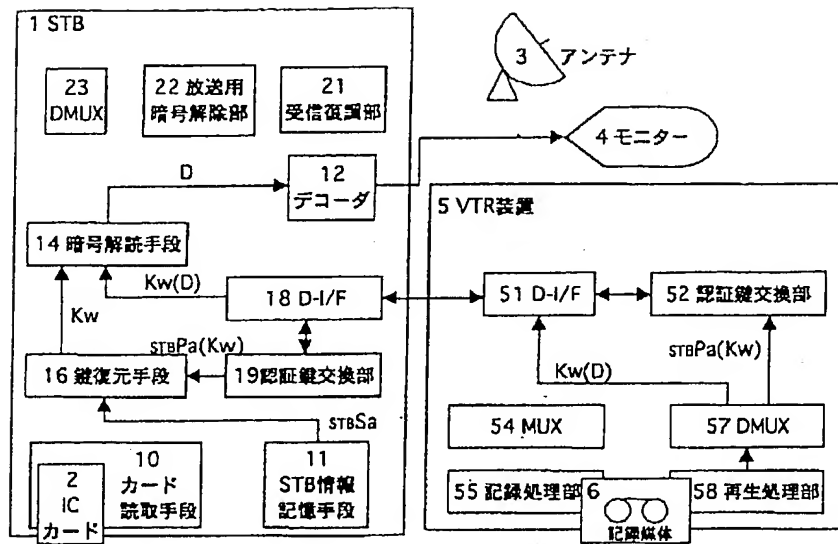
【図1】



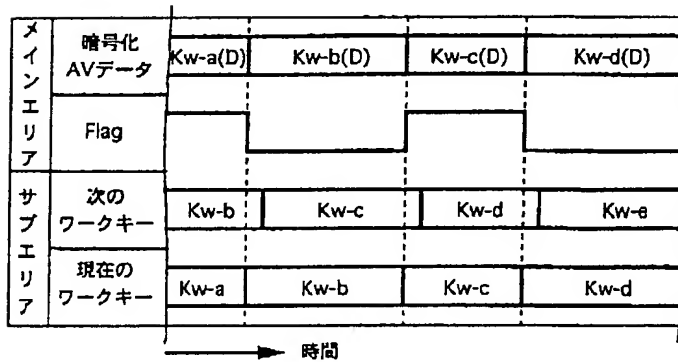
【図2】



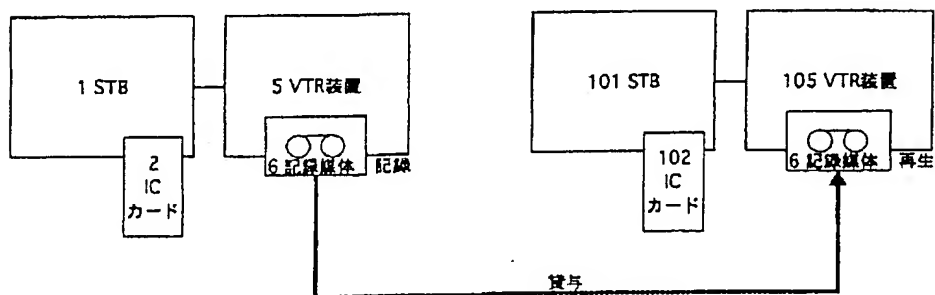
【図3】



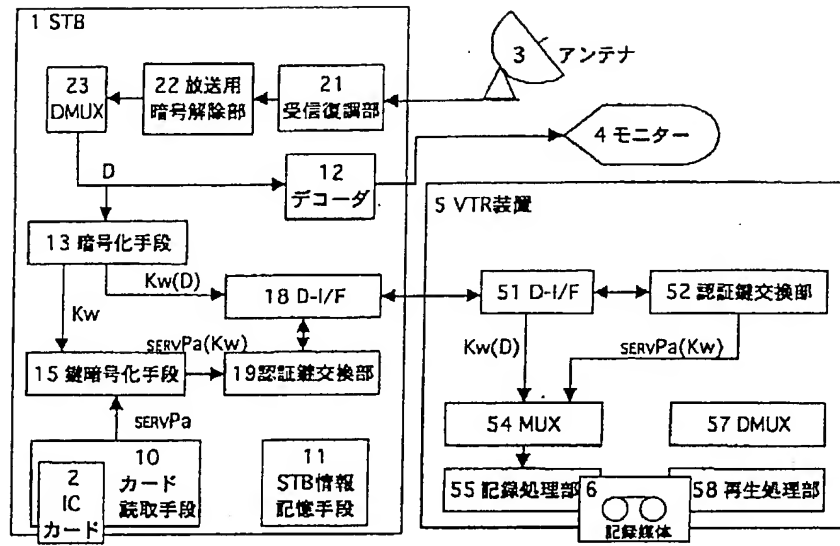
【図4】



【図5】



【図8】



【図9】

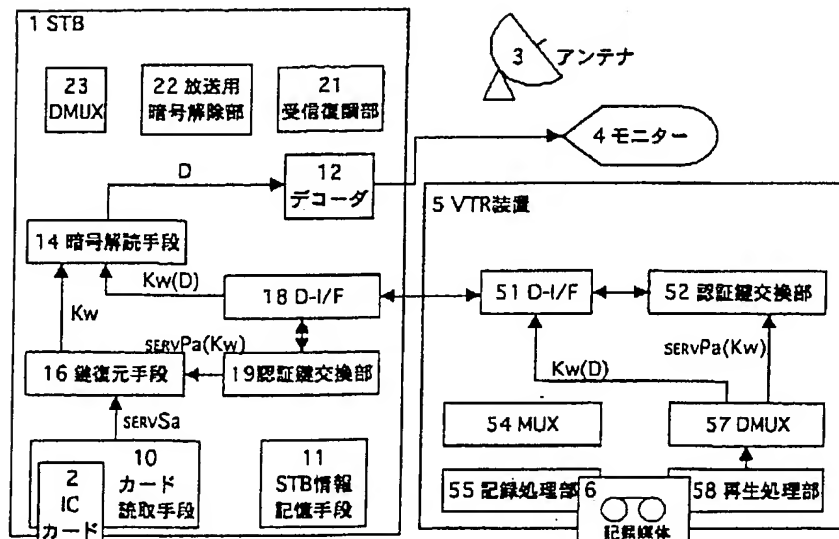


Figure 1 is a block diagram of a video recording system. The system includes an antenna (3) connected to a 1STB (1) and a 5 VTR device (5). The 1STB (1) contains a reception section (20) with a DMUX (23), a descrambler (22), and a tuner (21). It also includes a decoder (12), a scrambling section (13), a descrambling section (14), a scrambling section (31), a descrambling section (16), an IC card (2), a card reading section (10), a VTR transport section (17), a D-I/F (18), a scrambling section (19), and an STB information storage section (11). The 5 VTR device (5) contains a descrambling section (61), an STB transport section (50), a scrambling section (52), a D-I/F (51), a recording section (53), a MUX (54), a recording processing section (55), a regeneration section (56), a DMUX (57), and a regeneration processing section (58). A monitor (4) is connected to the system. A recording medium (6) is also shown.

Figure 1 is a block diagram of a video recording system. The system is divided into two main sections: a left section for STB (1 STB) and a right section for VTR (5 VTR装置).

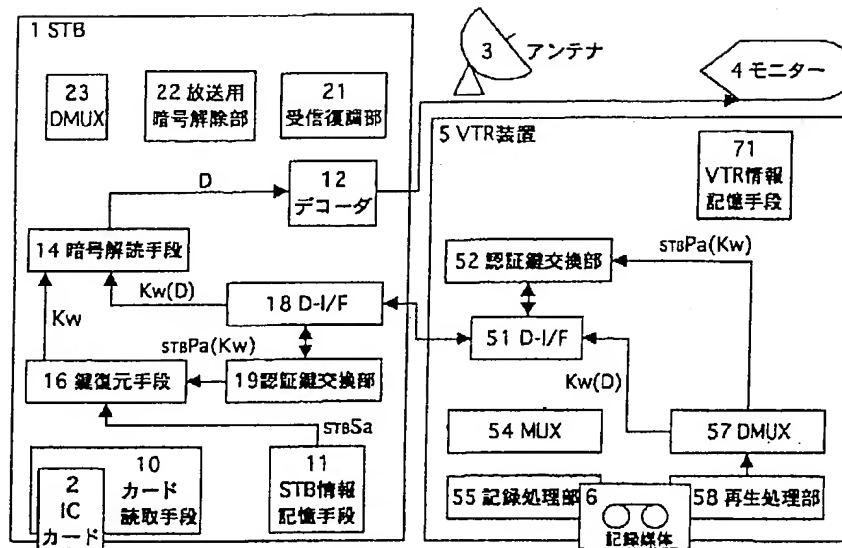
1 STB Section:

- 21 受信復調部** (Receiving/De-modulation Section) receives signals from the antenna (3) and outputs to **22 放送用暗号解除部** (Broadcasting Cryptography Removal Section) and **12 デコーダ** (Decoder).
- 22 放送用暗号解除部** outputs to **23 DMUX** (Demultiplexer).
- 23 DMUX** outputs **D** to **13 暗号化手段** (Encryption Means) and **Kw(D)** to **18 D-I/F** (Digital Interface).
- 13 暗号化手段** outputs **Kw** to **31 鍵暗号化手段** (Key Encryption Means).
- 31 鍵暗号化手段** outputs **Kc(Kw)** to **19 認証鍵交換部** (Authentication Key Exchange Section).
- 19 認証鍵交換部** outputs **Kc** to **11 STB情報記憶手段** (STB Information Storage Means) and **Kc(Kw)** to **18 D-I/F**.
- 18 D-I/F** outputs to **51 D-I/F** (Digital Interface) in the VTR section.
- 2 ICカード** (IC Card) and **10 カード読取手段** (Card Reading Means) are connected to the system.

5 VTR装置 Section:

- 3 アンテナ** (Antenna) receives signals from the STB section and outputs to **51 D-I/F** and **71 VTR情報記憶手段** (VTR Information Storage Means).
- 4 モニター** (Monitor) receives signals from the antenna.
- 71 VTR情報記憶手段** outputs **Kc** to **61 鍵復元手段** (Key Restoration Means) and **stPa** to **62 鍵暗号化手段** (Key Encryption Means).
- 61 鍵復元手段** outputs **Kc(Kw)** to **52 認証鍵交換部** (Authentication Key Exchange Section).
- 52 認証鍵交換部** outputs **Kw** to **61 鍵復元手段** and **stPa(Kw)** to **62 鍵暗号化手段**.
- 62 鍵暗号化手段** outputs **stPa(Kw)** to **54 MUX** (Multiplexer).
- 51 D-I/F** outputs **Kw(D)** to **54 MUX**.
- 54 MUX** outputs to **55 記録処理部** (Recording Processing Section) and **57 DMUX** (Demultiplexer).
- 55 記録処理部** outputs to **6 記録媒体** (Recording Medium).
- 57 DMUX** outputs to **58 再生処理部** (Reproduction Processing Section).
- 6 記録媒体** (Recording Medium) outputs to **58 再生処理部**.

【図12】



【図13】

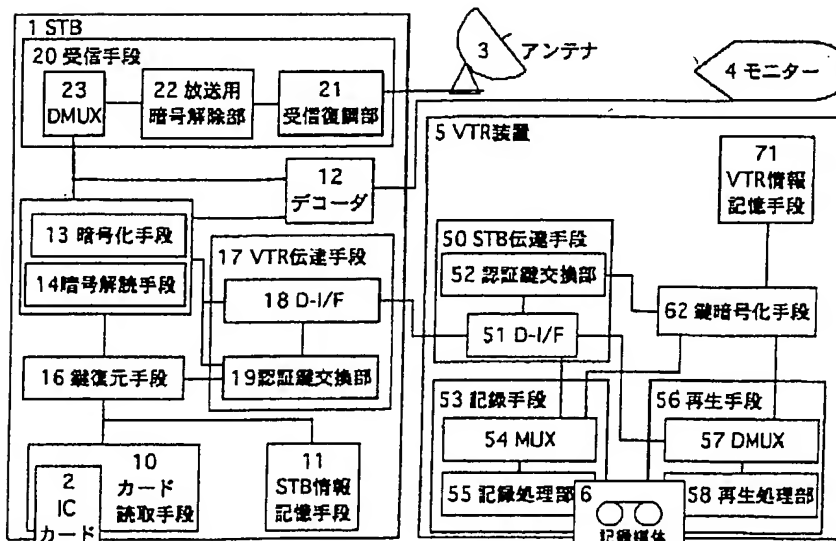
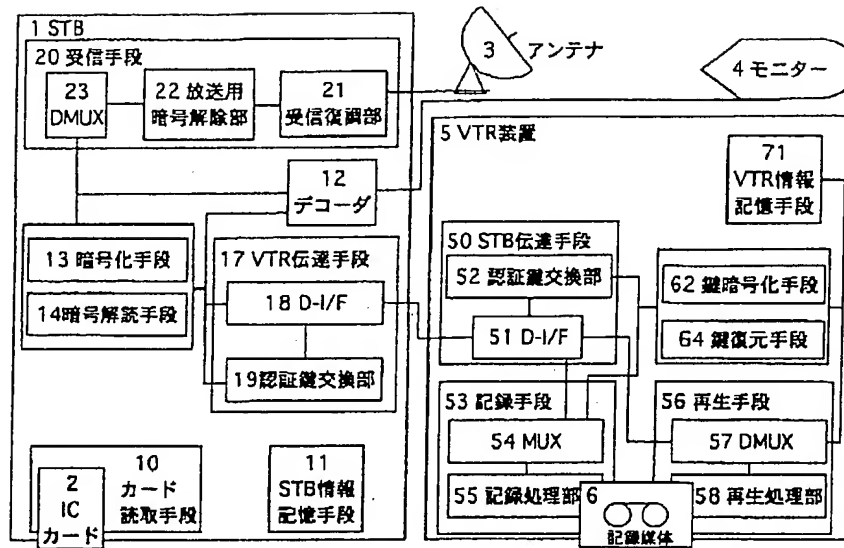


Figure 1 is a block diagram of a 1STB system. The system is divided into two main sections: 1STB (1) and 5VTR装置 (5). The 1STB (1) section includes a 2 ICカード (2), 10 カード読取手段 (10), 11 STB情報記憶手段 (11), 12 デコーダ (12), 13 暗号化手段 (13), 18 D-I/F (18), 19 認証鍵交換部 (19), 21 受信復調部 (21), 22 放送用暗号解除部 (22), and 23 DMUX (23). The 5VTR装置 (5) section includes a 51 D-I/F (51), 52 認証鍵交換部 (52), 54 MUX (54), 55 記録処理部 (55), 57 DMUX (57), 58 再生処理部 (58), 62 鍵暗号化手段 (62), and 71 VTR情報記憶手段 (71). An antenna (3) is connected to the 1STB (1) and the 5VTR装置 (5). A monitor (4) is connected to the antenna (3). Data flows are indicated by arrows: D from 23 to 12, Kw(D) from 13 to 18, Kw from 13 to 19, STBPa from 71 to 62, Kw from 52 to 62, STBPa(Kw) from 62 to 51, Kw(D) from 51 to 54, and a recording signal from 54 to 55. A recording medium (記録媒体) is connected to the 55 記録処理部 (55).

Figure 1 is a block diagram of a video recording system. The system includes an antenna (3) connected to an STB (1) and a monitor (4). The STB (1) contains a 20 receiving section with a 23 DMUX, 22 descrambler, and 21 tuner. It also includes a 12 decoder, 13 scrambling section, 14 descrambler, 31 scrambling section, 32 descrambler, 2 IC card, 10 card access section, 11 STB information storage section, and 17 VTR transmission section. The VTR (5) contains a 51 D-I/F, 50 STB transmission section, 52 scrambling section, 53 recording section, 54 MUX, 55 recording processing section, 61 descrambler, 63 scrambling section, 62 scrambling section, 64 descrambler, 56 reproduction section, 57 DMUX, 58 reproduction processing section, 71 VTR information storage section, and 72 VTR control section. The system also includes a 6 recording body.

【図18】



【図19】

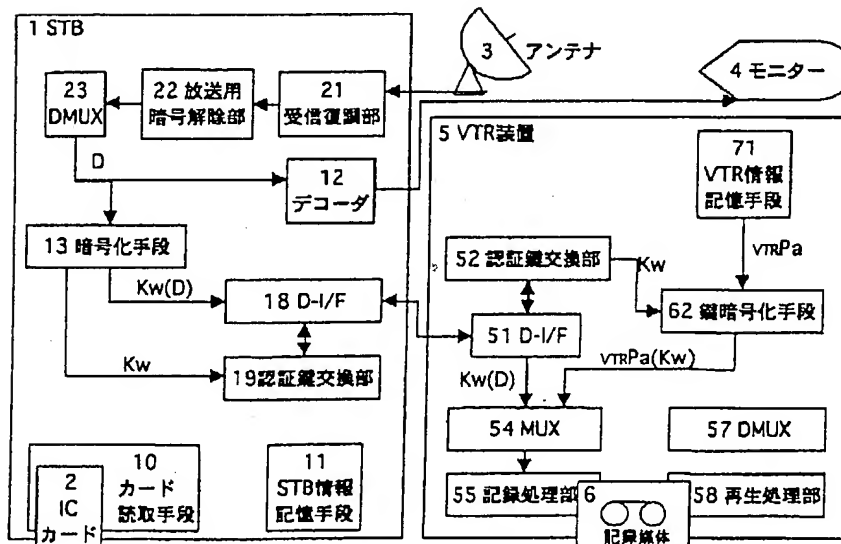


図1

1 STB

2 ICカード

10 カード読取手段

11 STB情報記憶手段

12 デコーダ

14 暗号解読手段

18 D-I/F

19 認証鍵交換部

23 DMUX

22 放送用暗号解除部

21 受信復調部

3 アンテナ

4 モニター

5 VTR装置

51 D-I/F

52 認証鍵交換部

54 MUX

55 記録処理部

57 DMUX

58 再生処理部

64 復元手段

71 VTR情報記憶手段

72 記録媒体

D

Kw(D)

Kw

vtrSa

Kw

Kw(D)

VTRPa(Kw)

V

1 STB (Set-Top Box):

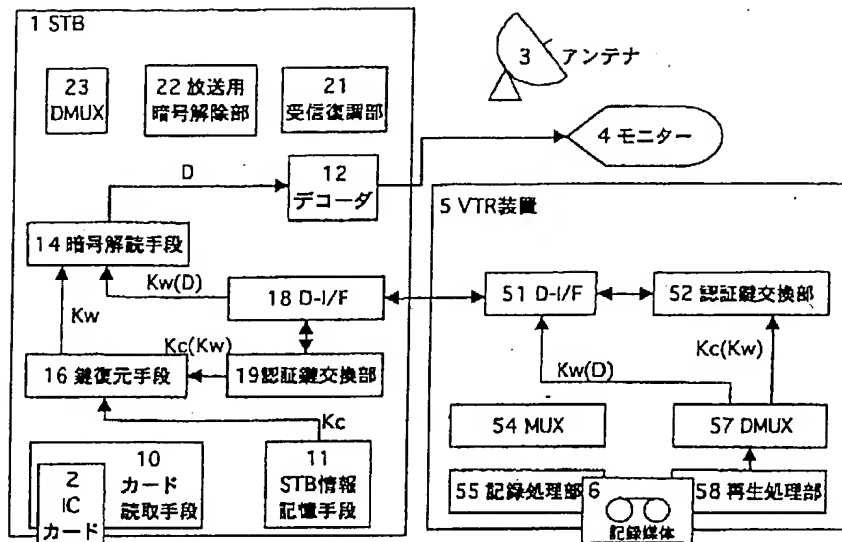
- 23 DMUX:** Receives signals from the antenna and outputs signal **D** to the decoder and signal **Kw** to the scrambling section.
- 22 放送用暗号解除部 (Broadcast Decryption Section):** Receives signals from the antenna and outputs to the DMUX.
- 21 受信復調部 (Reception Demodulation Section):** Receives signals from the antenna and outputs to the decryption section.
- 12 デコーダ (Decoder):** Receives signal **D** and outputs to the monitor.
- 13 暗号化手段 (Scrambling Means):** Receives signal **Kw** and outputs to the scrambling section.
- 15 鍵暗号化手段 (Key Scrambling Means):** Receives signal **Kc(Kw)** and outputs to the scrambling section.
- 18 D-I/F (Data Interface):** Receives signal **Kw(D)** and outputs to the scrambling section.
- 19 認証鍵交換部 (Authentication Key Exchange Section):** Receives signal **Kc** and outputs to the scrambling section.
- 2 ICカード (IC Card):** Connected to the scrambling section.
- 10 カード読取手段 (Card Reading Means):** Connected to the scrambling section.
- 11 STB情報記憶手段 (STB Information Storage Means):** Connected to the scrambling section.

5 VTR装置 (VCR Device):

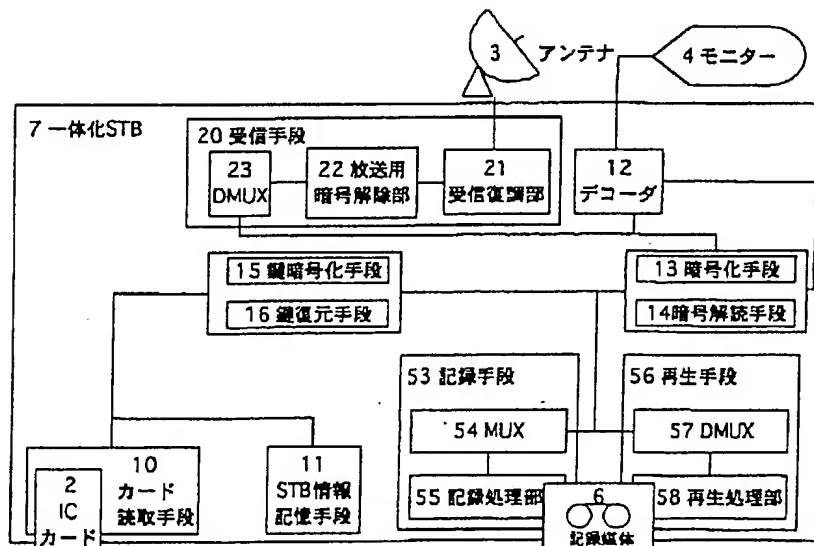
- 51 D-I/F (Data Interface):** Receives signal **Kw(D)** and outputs to the MUX.
- 52 認証鍵交換部 (Authentication Key Exchange Section):** Receives signal **Kc(Kw)** and outputs to the MUX.
- 54 MUX (Multiplexer):** Receives signals from the D-I/F and the scrambling section, and outputs to the recording section.
- 55 記録処理部 (Recording Processing Section):** Receives signals from the MUX and the recording medium.
- 57 DMUX (Demultiplexer):** Receives signals from the recording section and outputs to the playback section.
- 58 再生処理部 (Playback Processing Section):** Receives signals from the DMUX and outputs to the monitor.
- 記録媒体 (Recording Medium):** Connected to the recording and playback sections.

Antenna (3 アンテナ) and Monitor (4 モニター): The antenna receives signals from the broadcast station. The monitor displays the output from the decoder and the playback section.

【図22】



【図23】



The diagram illustrates the internal architecture of a 7-in-1 STB. At the top, an antenna (3) receives signals and sends them to a monitor (4). The main processing is contained within a box labeled '7 一体化STB'. Inside, the signal path starts with a receiving tuner (21) and a decoder (12). The decoder (12) outputs to a demultiplexer (23) and also provides a data stream 'D' to a recording encoder (13). The recording encoder (13) outputs a signal 'Kw' to a recording decoder (15). The recording decoder (15) outputs to a demultiplexer (23) and also provides a signal 'stbPa' to a card information memory (11). The card information memory (11) outputs to a card (2) and a card extraction unit (10). The recording encoder (13) also outputs a signal 'Kw(D)' to a multiplexer (54). The multiplexer (54) outputs to a recording processor (55). The recording processor (55) outputs to a recording medium (6). The recording medium (6) outputs to a reproduction processor (58). The reproduction processor (58) outputs to a demultiplexer (57). The demultiplexer (57) outputs to a multiplexer (54) and also provides a signal 'stbPa(Kw)' to the recording decoder (15).

7 一体化STB

23 DMUX

22 放送用
暗号解除部

21 受信復調部

12 デコーダ

16 復元手段

14 暗号解読手段

54 MUX

55 記録処理部

57 DMUX

58 再生処理部

6 記録媒体

10 カード
読取手段

2 IC
カード

11 STB情報
記憶手段

3 アンテナ

4 モニター

D

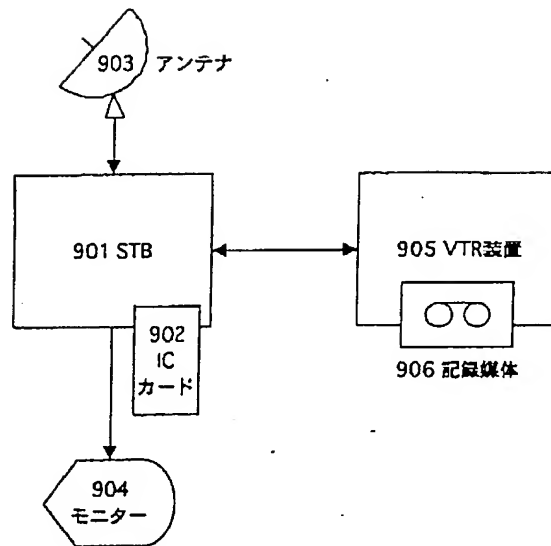
Kw

STBPa(Kw)

STBSa

Kw(D)

【図26】



フロントページの続き

(72)発明者 武知 秀明
大阪府門真市大字門真1006番地 松下電器
産業株式会社内